Chen G, Tian Z, Gong Y, Zhi C, Chambers JA.

Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks.

***IEEE Transactions on Information Forensics and Security* 2014, 9(4), 719-729**

DOI link to article:

http://dx.doi.org/10.1109/TIFS.2014.2307672

Date deposited:

08/02/2017

Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks

Gaojie Chen, *Member, IEEE*, Zhao Tian, *Student Member, IEEE,* Yu Gong, *Member, IEEE*, Zhi Chen, *Member, IEEE* and Jonathon Chambers, *Fellow, IEEE*

***Abstract*—This paper considers the security of transmission in buffer-aided decode-and-forward cooperative wireless networks. An eavesdropper which can intercept the data transmission from both the source and relay nodes is considered to threaten the security of transmission. Finite size data buffers are assumed to be available at every relay in order to avoid having to select concurrently the best source-to-relay and relay-to-destination links. A new max-ratio relay selection policy is proposed to optimize the secrecy transmission by considering all the possible source-to-relay and relay-to-destination links and selecting the relay having the link which maximizes the signal to eavesdropper channel gain ratio. Two cases are considered in terms of knowledge of the eavesdropper channel strengths: exact and average gains, respectively. Closed-form expressions for the secrecy outage probability for both cases are obtained, which are verified by simulations. The proposed max-ratio relay selection scheme is shown to outperform one based on a max-min-ratio relay scheme.**

***Index Terms*—Secure wireless communications, cooperative networks, relay selection, secrecy capacity.**

I. Introduction

TRADITIONALLY security in wireless networks has been focused on higher layers using cryptographic methods [1]. However, retaining security at high layers is becoming more challenging due to the increased potential for attack, therefore, there has been growing interest in implementing security at the physical layer. Related work was described as early as in the 1970s [2]–[5], and more recently for physical layer security in wireless communications [6]–[10]. The purpose of physical layer security is to prevent eavesdroppers from intercepting the data transmitted between the source and intended destination. The secrecy is quantified by the secrecy capacity, or the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers [5].

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) Grant number EP/K014307/1 and the MOD University Defence Research Collaboration in Signal Processing.

G. J. Chen, Z. Tian, Y. Gong and J. A. Chambers are with the Advanced Signal Processing Group, School of Electronic, Electrical and Systems Engineering, Loughborough University, Loughborough, Leicestershire, UK, Emails: {g.chen, z.tian, y.gong, j.a.chambers}@lboro.ac.uk.

Z. Chen is with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China, E-mail: chenzhi@uestc.edu.cn.

Recent research shows that cooperative communication not only significantly improves the transmission capacity for wireless networks (e.g. [11], [12]), but also provides an effective way to improve the secrecy capacity. This is achieved by carefully designing the relays to maximize the information rate at the intended destination and minimize that at the eavesdroppers [13]. In general, there are three ways to improve the secrecy capacity in a cooperative network:

- *Distributed beamforming* - The secrecy capacity can be maximized by optimizing the transmission weights (or the beamforming weights) at the relay and source nodes (e.g. [14], [15]). Such distributed beamforming however requires high coordination (such as synchronization and central optimization) among source and relay nodes, which usually requires high overhead in implementation, i.e. a large amount of information needs to be exchanged between the relay nodes.
- *Jamming* - A jammer is used to inject artificial interference into the system. When the injected interfering power is higher at the eavesdroppers than that at the intended destination, the secrecy capacity can be improved (e.g. [16]–[18]). This often requires the jammer to be located closer to the eavesdroppers than to the destination node, which is not always possible in practice.
- *Relay selection* - Relay selection can increase the secrecy capacity by choosing an appropriate relay node with "strong" transmission link to the intended destination node and "weak" link to the eavesdropper [19]–[22]. The relay selection provides an attractive way to improve the secrecy capacity with little overhead in implementation. The performance of the relay selection depends strongly on the number of available links for selection, which again depends on not only the number of relays but also the relay selection scheme. When the number of available links is limited, so is the secrecy performance. Thus it is important to investigate relay selection schemes to have the best secrecy performance for a given number of relays, which is the main objective of this paper.

In traditional relay selection to improve wireless communications, the best relay is selected with the strongest link connecting the source and destination (e.g. [23], [24]). It is shown in [19] that by using relay selection the secrecy capacity can also be improved when the best relay is selected to maximize the signal to eavesdropper channel gain ratio, which is abbreviated as the "gain ratio" in this paper. The relay selection scheme in [19] is based on the scenario that

the eavesdropper can only intercept the signals from the relays but not the source node. On the other hand, if the eavesdropper intercepts signals from both the relay and source nodes, the best relay is selected as having the maximum secrecy capacity among every pair of source-to-relay and relay-to-destination links [18], which is termed as the *max-min-ratio* scheme in this paper. Alternatively, it is also possible to select a jammer from the available relays (e.g [20]), but this is at the price of injecting more inference not only to the intended receivers but also to other users in the system. As was shown in [20], including a jammer does not necessarily lead to improvement in secrecy capacity, and thus a switching scheme was described to activate/deactivate the jammer.

Recent research shows that, by introducing data buffers at the relays, it is possible to relax the constraint that the best source-to-relay and relay-to-destination links for a packet transmission must be determined concurrently, and achieve significant performance advantage [25]–[30]. A typical buffer-aided relay selection is the *max-max* scheme described in [27], where the strongest source-to-relay and relay-to-destination links are selected alternatively so that it has significant coding gain over the traditional *max-min* scheme. Because the *max-max* relay selection still follows the traditional transmission order, that is the source-to-relay and relay-to-destination transmissions always carry on in an alternative manner, it can only attain a diversity order of N which is the same as that for the *max-min* scheme, where N is the number of available relay nodes. In the recent *max-link* approach [25], this constraint on the transmission order is further relaxed so that, at any time, a best link is selected among all available source-to-relay and relay-to-destination links. Depending on whether a source-to-relay or a relay-to-destination link is selected, either the source transmits a packet to the selected relay or the selected relay forwards a stored packet to the destination. It is shown in [25] that the *max-link* relay selection not only has coding gain over the *max-min* scheme, but also has higher diversity order than both the *max-min* and *max-max* schemes. In particular, the diversity order can approach $2N$ when the relay buffer size is large enough.

Inspired by the max-link scheme, in this paper, we propose a novel *max-ratio* relay selection scheme for secure transmission in decode-and-forward (DF) relay networks with an eavesdropper which can intercept signals from both the source and relay nodes. In the proposed *max-ratio* scheme, every relay is equipped with a data buffer, and the best link is always selected with the highest gain ratio among all available source-to-relay and relay-to-destination links. We consider two cases for which either the exact, or the average gain, for the eavesdropping channel is available; the latter case is of particular interest in practice since it is not always possible to obtain the exact channel information describing the eavesdropping channels. Both theoretical and simulation results show that the proposed max-ratio relay selection has significantly better performance than the conventional max-min-ratio scheme, confirming that it represents an attractive approach for secure wireless transmission. The main contributions of this paper are summarized as follows to:

- *Propose the buffer-aided max-ratio relay selection policy for secure communications in a DF cooperative network*. This is the first approach in using buffer-aided relay selection in secure transmission under the scenario that the eavesdropper can intercept signals from both the source and relay nodes. Existing relay selection schemes for secure transmission mainly assume no source-to-eavesdropper link for simplicity (e.g. [19]). While in [22] both the source and relay to eavesdropper links are considered, the proposed scheme is for the two-way relay network and furthermore no closed form expression is obtained for the secrecy outage probability.
- *Derive closed-form expressions for the secrecy outage probability of the max-ratio scheme for both cases when either the exact, or average, gains of the eavesdropping channels are available*. Because the gain-ratios for the source-to-relay and relay-to-destination transmissions have different statistical distributions, the secrecy outage performance of the proposed max-ratio scheme is much more involved to analyze than existing approaches such as the relay selection scheme for secure transmission in [19] and the buffer-aided max-link scheme for wireless communications in [25]. In this paper, the problem arising from such "unbalanced" distribution has been successfully solved, and the analysis also provides a useful way in analyzing similar systems such as a typical relay selection scheme but without the usual assumption that the source-to-relay and relay-to-destination channels are independent and identically distributed (i.i.d.).

The remainder of the paper is organized as follows: Section II describes the system model; Section III proposes the max-ratio relay selection scheme; Sections IV and V analyze the secrecy outage probability for the cases with exact and average knowledge of the eavesdropping channels, respectively; Section VI discusses the performance of the max-ratio scheme when the relay buffer sizes go to infinity; Section VII gives numerical simulations to verify the proposed max-ratio scheme; finally, Section VIII summarizes the paper.

II. System Model

The system model of the relay network with an eavesdropper is shown in Fig. 1, where there is one source node (S), one destination node (D), a set of K relays $\{R_1, R_2, ..., R_K\}$, and one eavesdropper (E) which can intercept signals from both the source and relay nodes. The relay nodes apply the DF protocol and perform the half-duplex mode so that they do not transmit and receive simultaneously.

In our model, we assume no direct link between the source and the destination due to path loss or shadowing effects[1]. The channel coefficients for $S \to R_k$, $S \to E$, $R_k \to D$ and $R_k \to E$ at time t are denoted as $h_{sr_k}(t)$, $h_{se}(t)$, $h_{r_kd}(t)$ and $h_{r_ke}(t)$ respectively, where similar subscripts are also used for other parameters to indicate different channels in this paper. We assume the channels are quasi-static Rayleigh fading so that the channel coefficients remain unchanged during one packet duration but independently vary from one

[1]Including the direct link has little effect on the relay selection which is the main issue in this paper.

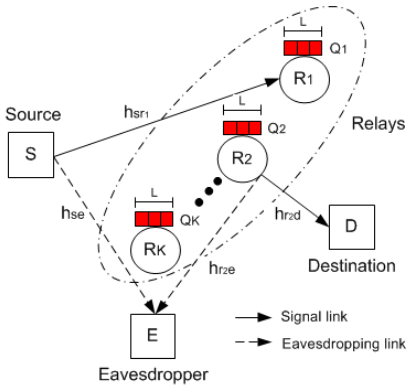


Fig. 1. Relay selection system model in secure transmission, where the eavesdropper intercepts signals from both the source and relay nodes.

packet time to another. We also assume that all source-to-relay links are independent and identically distributed (i.i.d.) fading and that $\mathrm{E}|h_{sr_k}(t)|^2 = \gamma_{sr}$ for all k; all relay-to-destination channel gains are also i.i.d. and $\mathrm{E}|h_{r_kd}(t)|^2 = \gamma_{rd}$, as are all relay-to-eavesdropper channel gains for which $\mathrm{E}|h_{r_ke}(t)|^2 = \gamma_{re}$. The source-to-eavesdropper channel gain is denoted as $\mathrm{E}|h_{se}(t)|^2 = \gamma_{se}$. It is noted that we do not require any two of γ_{sr}, γ_{rd}, γ_{se} and γ_{re} to be the same, thereby representing a "practical" scenario. All noises are additive white Gaussian noise (AWGN), and without losing generality the noise variances are all normalized to unity. The transmission powers for source and relay nodes are all assumed to be E_s.

With the DF applied at the relays, if the relay R_k is selected for the data transmission, the instantaneous secrecy capacity for the overall system is obtained as [31]

$$C_k(t) = \max\left\{\frac{1}{2}\log_2\frac{\min\{1+E_s|h_{sr_k}(t)|^2, 1+E_s|h_{r_kd}(t)|^2\}}{1+E_s|h_{se}(t)|^2+E_s|h_{r_ke}(t)|^2}\right\} \quad (1)$$

If the exact knowledge of the eavesdropping channels are available, the best relay node can be selected with the maximum $C_k(t)$. On the other hand, if only the average gains of the eavesdropping channels are known, the best relay maximizes $C_k(t)$ with $|h_{se}(t)|^2$ and $|h_{r_ke}(t)|^2$ being replaced with the average gains γ_{se} and γ_{re} in (1) respectively. This scheme is termed as the max-min-ratio relay selection in this paper.

For convenience in development, the time index t is ignored in the rest of the paper unless necessary.

III. Max-ratio relay selection

The performance of the max-min-ratio scheme is limited by the constraint that the best source-to-relay and relay-to-destination links must be determined concurrently. In this paper, we propose a new max-ratio selection scheme by making use of data buffers at the relays. To be specific, we assume that every relay is equipped with a data buffer Q_k $(1 \le k \le K)$ of finite size L (in the number of data packets), and the data packets in the buffer follow the "first-in-first-out" rule. At any time, the best transmission link with the highest gain-ratio is selected among all available source-to-relay and relay-to-destination links. Depending on the knowledge of the eavesdropper channel, we have two selection criteria:

Case 1 - If the exact knowledge of all channels[2], including the eavesdropping channels h_{se} and h_{r_ke}, are available, the max-ratio selects the best relay as

$$R_{case\ 1}^{(max-ratio)} = \arg\max_{R_k}\left\{\frac{\max\limits_{R_k:\Psi(Q_k)\neq L}\{|h_{sr_k}|^2\}}{|h_{se}|^2}, \max_{R_k:\Psi(Q_k)\neq 0}\left\{\frac{|h_{r_kd}|^2}{|h_{r_ke}|^2}\right\}\right\}, \quad (2)$$

where $\Psi(Q_k)$ gives the number of data packets in buffer Q_k.

Case 2 - If only the average channel gains for the eavesdropping channels, i.e. γ_{se} and γ_{re}, are available (but the exact knowledge for all other channels is known), the best relay for the max-ratio scheme is selected as:

$$R_{case\ 2}^{(max-ratio)} = \arg\max_{R_k}\left\{\frac{\max\limits_{R_k:\Psi(Q_k)\neq L}\{|h_{sr_k}|^2\}}{\gamma_{se}}, \frac{\max\limits_{R_k:\Psi(Q_k)\neq 0}\{|h_{r_kd}|^2\}}{\gamma_{re}}\right\}. \quad (3)$$

A. Secrecy outage probability

The secrecy outage probability is defined as $P_{out} = P(C < r_{sc})$, where C is the instantaneous secrecy capacity, r_{sc} is the target secrecy capacity and $P(.)$ gives the probability of the enclosed. In the max-ratio relay selection scheme, at any time, the numbers of data packets in every buffer form a "state". Because there are K available relays and every relay is equipped with a buffer of size L, there are $(L+1)^K$ states in total. The l-th state vector is defined as

$$\mathbf{s}_l = [\Psi_l(Q_1), \cdots, \Psi_l(Q_K)]^{\mathrm{T}}, \qquad l = 1, \cdots, (L+1)^K, \quad (4)$$

where $\Psi_l(Q_k)$ gives the number of data packets in buffer Q_k at state s_l. It is clear that $0 \le \Psi_l(Q_k) \le L$. Every state corresponds to one pair of (K_1, K_2), where K_1 and K_2 are the numbers of available links for source-to-relay and relay-to-destination transmission, respectively. A source-to-relay or a relay-to-destination link is considered available when the buffer of the corresponding relay node is not full or not empty respectively. It is clear that $0 \le K_1 \le K$ and $0 \le K_2 \le K$. Specifically, if none of the buffers is full or empty, all links are available such that $K_1 = K_2 = K$.

At state s_l, the best link is selected among all K_1 source-to-relay and K_2 relay-to-destination links. We denote $p_{out}^{s_l}$ as the outage probability for state s_l. Considering all possible states, we obtain the secrecy outage probability for the max-ratio relay selection as

$$P_{out} = \sum_{l=1}^{(L+1)^K} \pi_l \cdot p_{out}^{s_l}, \quad (5)$$

where $\pi_l = p(s_l)$ which is the stationary probability for state s_l.

[2]The CSI is usually estimated through pilots and feedback (e.g. [32]), and the CSI estimation without feedback may also be applied (e.g [33]). Further detail of the CSI estimation is beyond the scope of this paper.

B. State transition matrix

Suppose at time t, the state for the relay buffers is s_l. At time $(t+1)$, there is one relay selected for either receiving or transmitting a data packet, so that the number of packets in the corresponding buffer is increased or decreased by one respectively. Depending on which relay receives or transmits data, at time $(t+1)$, the buffers may move from state s_l to several possible states, forming a Markov chain. We denote $\mathbf{A}$ as the $(L+1)^K \times (L+1)^K$ state transition matrix, where the entry $\mathbf{A}_{n,l} = P(X_{t+1} = s_n | X_t = s_l)$ is the transition probability that the state moves from s_l at time t to s_n at time $(t+1)$.

If the secrecy outage event occurs, the state s_l remain unchanged at time $(t+1)$. Otherwise, s_l moves to another state. Thus the probability for s_l to leave for another state is given by

$$p_{s_l}^{\text{leave}} = 1 - p_{out}^{s_l}. \tag{6}$$

It is clear from the selection rules (2) and (3) that, for both Cases 1 and 2, the probabilities to select the source-to-relay and relay-to-destination transmission at any time are not the same. This is very different from the max-link approach in [25] where the selection of any available link is equally likely. We divide all states which can be moved from s_l into two sets, U_l^+ and U_l^-, where U_l^+ contains all states to which s_l can move when a source-to-relay link is selected and U_l^- contains all states to which s_l can move when a relay-to-destination link is selected. We let $p_{s_l}^{S\to D}$ and $p_{s_l}^{R\to D}$ be the probabilities that the source-to-relay and relay-to-destination transmissions are selected at state s_l, respectively. It is clear that $p_{s_l}^{S\to D} + p_{s_l}^{R\to D} = 1$.

On the other hand, because we assume all source-to-relay channels are i.i.d. fading and all relay-to-destination channels are also i.i.d. frequency flat fading and so are the relay-to-eavesdropper channels, the selection of one particular link within either U_l^+ or U_l^- is equally likely. Therefore, the probability to select a source-to-relay or relay-to-destination link at state s_l is given by

$$\begin{aligned} p_{s_l}^{+} &= p_{s_l}^{\text{leave}} \left(\frac{1}{K_1} \; p_{s_l}^{S\to R} \right) = \frac{1}{K_1}(1 - p_{out}^{s_l})(1 - p_{s_l}^{R\to D}), \\ p_{s_l}^{-} &= p_{s_l}^{\text{leave}} \left(\frac{1}{K_2} \; p_{s_l}^{R\to D} \right) = \frac{1}{K_2}(1 - p_{out}^{s_l}) p_{s_l}^{R\to D}, \end{aligned} \tag{7}$$

respectively.

With these observations, the (n,l)-th entry of the state transition matrix $\mathbf{A}$ is expressed as

$$\mathbf{A}_{n,l} = \begin{cases} \overline{p}_{s_l} = p_{out}^{s_l}, & \text{if} \quad n = l, \\ p_{s_l}^{+} = \frac{1}{K_1}(1 - p_{out}^{s_l})(1 - p_{s_l}^{R\to D}), & \text{if} \quad s_n \in U_l^+, \\ p_{s_l}^{-} = \frac{1}{K_2}(1 - p_{out}^{s_l}) p_{s_l}^{R\to D}, & \text{if} \quad s_n \in U_l^-, \\ 0, & \text{elsewhere}, \end{cases} \tag{8}$$

Because the transition matrix $\mathbf{A}$ in (8) is column stochastic, irreducible and aperiodic[3], the stationary state probability vector is obtained as (see [35], [36])

$$\boldsymbol{\pi} = (\mathbf{A} - \mathbf{I} + \mathbf{B})^{-1}\mathbf{b}, \tag{9}$$

where $\boldsymbol{\pi} = [\pi_1, \cdots, \pi_{(L+1)^K}]^{\mathrm{T}}$, $\mathbf{b} = (1, 1, ..., 1)^T$, $\mathbf{I}$ is the identity matrix and $\mathbf{B}_{n,l}$ is an $n \times l$ all one matrix.

Finally, substituting (8) and (9) into (5) re-formats the secrecy outage probability as

$$\begin{aligned} P_{out} &= \sum_{l=1}^{(L+1)^K} \pi_l \cdot p_{out}^{s_l} = \text{diag}(\mathbf{A}) \cdot \boldsymbol{\pi} \\ &= \text{diag}(\mathbf{A}) \cdot (\mathbf{A} - \mathbf{I} + \mathbf{B})^{-1}\mathbf{b}, \end{aligned} \tag{10}$$

where $\text{diag}(\mathbf{A})$ is a vector consisting of all diagonal elements of $\mathbf{A}$.

It is clear from (10) that the secrecy outage probability P_{out} is determined by $\mathbf{A}$ which again, from (8), is determined by $p_{out}^{s_l}$ and $p_{s_l}^{R\to D}$. The secrecy outage probabilities for both Cases 1 and 2 can be expressed as (10), but with different $p_{out}^{s_l}$ and $p_{s_l}^{R\to D}$ which are derived below.

IV. Case 1 - exact knowledge of eavesdropping channels

In Case 1, we assume exact knowledge for the instantaneous gains for all channels, including the eavesdropping channels. This is a typical assumption in many existing approaches (e.g. [20] and [21]).

A. $p_{out}^{s_l}$: outage probability at state s_l for Case 1

The relay selection rule for Case 1 is shown in (2). For better exposition, we let $x = \max\limits_{\Psi(Q_k)\neq L} \{|h_{sr_k}|^2\}/|h_{se}|^2$, $y = \max\limits_{\Psi(Q_k)\neq 0} \{|h_{r_kd}|^2/|h_{r_ke}|^2\}$ and $z = \max(x, y)$. In order to concentrate on the secrecy capacity, we assume the channel SNR is high enough so that the decoding is always successfully at the relay and destination nodes[4]. The probability of outage event at state s_l at the high SNR is given by

$$p_{out}^{s_l} = P(z < 2^{2r_{sc}}) = F_Z(z)|_{z=2^{2r_{sc}}}, \tag{11}$$

where $F_Z(z)$ is the cumulative-probability-function (CDF) of z which is derived below.

Recall that state s_l corresponds to (K_1, K_2). From the theory of order statistics [37], if the number of available source-to-relay links is K_1, the CDF of $x_1 = \max\limits_{\Psi(Q_k)\neq L} \{|h_{sr_k}|^2\}$ is given by

$$F_{X_1}(x) = [1 - e^{-\frac{x}{\gamma_{sr}}}]^{K_1}, \tag{12}$$

Noting that $x = x_1/|h_{se}|^2$, the CDF of x is then obtained as

$$F_X(x) = \sum_{i=0}^{K_1} C_{K_1}^i (-1)^i \frac{M_1}{ix + M_1}, \tag{13}$$

where $C_{K_1}^i = K_1!/[i!(K_1 - i)!]$ which is the binomial coefficient, and $M_1 = \gamma_{sr}/\gamma_{se}$ which is the average gain ratio between the source-to-relay and source-to-eavesdropper channels.

[3] *Column stochastic* means all entries in any column sum up to one, *irreducible* means that it is possible to move from any state to any state, and *aperiodic* means that it is possible to return to the same state at any steps [34], [35].

[4] This is a typical assumption in most existing secure communications literature (e.g. [19], [20]).

On the other hand, because the number of available relay-to-destination links is K_2, the CDF of y is given by

$$F_Y(y) = \left[\frac{y}{M_2+y}\right]^{K_2} \tag{14}$$

where $M_2 = \gamma_{rd}/\gamma_{re}$ which is the average gain ratio between the relay-to-destination and relay-to-eavesdropper channels.

Because x and y are mutually independent, from (13) and (14), the CDF of $z = \max(x, y)$ is obtained as:

$$F_Z(z) = F_X(z)F_Y(z) = \sum_{i=0}^{K_1} C_{K_1}^i (-1)^i \frac{M_1}{iz+M_1}\left[\frac{z}{M_2+z}\right]^{K_2}. \tag{15}$$

Substituting (15) into (11) gives

$$p_{out}^{s_l} = \sum_{i=0}^{K_1} C_{K_1}^i (-1)^i \frac{M_1}{i2^{2r_{sc}}+M_1}\left[\frac{2^{2r_{sc}}}{M_2+2^{2r_{sc}}}\right]^{K_2}. \tag{16}$$

The next subsection will provide the probability of selecting the relay to destination transmission at state s_l.

B. $p_{s_l}^{R\to D}$: probability of selecting the relay-to-destination transmission at state s_l for Case 1

If there are no relay-to-destination links available (or $K_2 = 0$), we have $p_{s_l}^{R\to D} = 0$. On the other hand, if there are no source-to-relay links available (or $K_1 = 0$), we have $p_{s_l}^{R\to D} = 1$. For other cases, $p_{s_l}^{R\to D}$ is obtained in Appendix I. In summary, we have obtained $p_{s_l}^{R\to D}$ in (17) in the top of the next page, where $\mathcal{B}(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt$ which is the Beta function and $\mathcal{F}_{2,1}(a,b,c,z)$ is the first hypergeometric function. Finally, substituting (16) and (17) into (10) gives the secrecy outage probability at the high SNR for Case 1.

V. Case 2 - knowledge of the average channel gains for eavesdropping channels

In case 2, we only have knowledge of the average gains for eavesdropping channels, while the exact information for all other channels are still available.

A. $p_{out}^{s_l}$: outage probability at state s_l for Case 2

We let $u_{ab} = |h_{ab}|^2/\gamma_{ab}$ be the normalized gain for channel h_{ab}, where $\{ab\} \in \{sr_k, se, r_kd, r_ke\}$. Because of the normalization, all u_{ab} have the same probability-density-distribution (PDF) as

$$f_U(u) = e^{-u}, \tag{18}$$

The selection rule in (3) can then be expressed as

$$R_b^{(2)} = \arg\max_{R_k}\left\{\max_{R_k:\Psi(Q_k)\neq L}\{M_1\cdot u_{sr_k}\}\ ,\ \max_{R_k:\Psi(Q_k)\neq 0}\{M_2\cdot u_{r_kd}\}\right\}, \tag{19}$$

where M_1 and M_2 are defined in (13) and (14), respectively.

We further let $f = \max_{R_k:\Psi(Q_k)\neq L}\{M_1\cdot u_{sr_k}\}$, $g = \max_{R_k:\Psi(Q_k)\neq 0}\{M_2\cdot u_{r_kd}\}$ and $w = \max\{f,g\}$. It is clear that w is directly obtained from the selection rule (3) which is based on the average gain of the eavesdropping channels. On the other hand, the secrecy outage is determined by the instantaneous gains of the data and eavesdropping channels. Therefore, in order to obtain the outage probability, w needs to be divided by u which is normalized exponentially distributed with PDF given by (18). Or the outage probability for state s_l for Case 2 is given by

$$p_{out}^{s_l} = P(v < 2^{2r_{sc}}) = F_V(v)|_{v=2^{2r_{sc}}}, \tag{20}$$

where $v = w/u$.

The CDF-s of f and g are given by

$$F_F(f) = \left[1-e^{-f/M_1}\right]^{K_1} \quad \text{and} \quad F_G(g) = \left[1-e^{-g/M_2}\right]^{K_2}, \tag{21}$$

respectively. Because f and g are mutually independent, the CDF of $w = \max\{f,g\}$ is obtained as

$$F_W(w) = F_F(w)F_G(w) = \left[1-e^{-w/M_1}\right]^{K_1}\left[1-e^{-w/M_2}\right]^{K_2}. \tag{22}$$

Then the CDF of $v = w/u$ is

$$\begin{aligned} F_V(v) &= \int_0^\infty \left[1-e^{-uv/M_1}\right]^{K_1}\left[1-e^{-uv/M_2}\right]^{K_2} e^{-u}du \\ &= \sum_{i=0}^{K_1}\sum_{j=0}^{K_2} C_{K_1}^i C_{K_2}^i (-1)^{i+j}\frac{M_1M_2}{v(M_2i+M_1j)+M_1M_2}. \end{aligned} \tag{23}$$

Substituting (23) into (11) gives

$$p_{out}^{s_l} = \sum_{i=0}^{K_1}\sum_{j=0}^{K_2} C_{K_1}^i C_{K_2}^i (-1)^{i+j}\frac{M_1M_2}{2^{2r_{sc}}(M_2i+M_1j)+M_1M_2}. \tag{24}$$

The next subsection will provide the probability of selecting the relay to destination transmission at state s_l.

B. $p_{s_l}^{R\to D}$: probability of selecting the relay-to-destination transmission at state s_l for Case 2

Similar to that in Case 1, we have $p_{s_l}^{R\to D} = 0$ for $K_2 = 0$, and $p_{s_l}^{R\to D} = 1$ for $K_1 = 0$. But otherwise, we have

$$p_{s_l}^{R\to D} = P(f < g) = \int\int_{f<g} f_{FG}(f,g)dfdg, \tag{25}$$

where $f_{FG}(f,g)$ is the joint PDF of f and g.

From (21), the PDFs of f and g are obtained as

$$\begin{aligned} f_F(f) &= \frac{K_1}{M_1}e^{-\frac{f}{M_1}}(1-e^{-\frac{f}{M_1}})^{K_1-1} \\ f_G(g) &= \frac{K_2}{M_2}e^{-\frac{g}{M_2}}(1-e^{-\frac{g}{M_2}})^{K_2-1}, \end{aligned} \tag{26}$$

respectively. Because f and g are mutually independent, we have $f_{FG}(f,g) = f_F(f)f_G(g)$.

Substituting (26) into (25) gives (27) in the top of the next page. Therefore, we have $p_{s_l}^{R\to D}$ in (28) in the top of the next page. Finally, substituting (24) and (28) into (10) gives the secrecy outage probability at high SNR for Case 2.

VI. Discussion

In this section, we consider a specific scenario that the average gain ratios for the source-to-relay and relay-to-destination transmissions are the same, or $M_1 = M_2$. Of particular interest

$$p_{s_l}^{R\to D}=\begin{cases}0, & K_2=0,\ 0<K_1\le K,\\ 1-K_1/2+\sum_{i=2}^{K_1}C_{K_1}^{i}(-1)^{i}\frac{i[\ln(i)-1]+1}{(i-1)^2}, & 0<K_1\le K,\ K_2=1, M_1=M_2\\ 1+\sum_{i=1}^{K_1}C_{K_1}^{i}(-1)^{i}M_1\frac{M_2 i\ln(i)+i\ln(M_2)M_2-i\ln(M_1)M_2-M_2 i+M_1}{(M_1-iM_2)^2}, & 0<K_1\le K, K_2=1, M_1\neq M_2\\ 1+\sum_{i=1}^{K_1}C_{K_1}^{i}(-1)^{i}K_2(\frac{M_1}{M_2 i})^{K_2}\mathcal{B}(2,K_2)\mathcal{F}_{2,1}([K_2+1,K_2],K_2+2,1-\frac{M_1}{M_2 i}), & 0<K_1\le K,\ 1<K_2\le K,\\ 1, & K_1=0,\ 0<K_2\le K,\end{cases} \tag{17}$$

$$p_{s_l}^{R\to D}=\int_0^{\infty}\int_0^{y}\frac{K_1K_2}{M_1M_2}e^{-\frac{x}{M_1}}e^{-\frac{y}{M_2}}(1-e^{-\frac{x}{M_1}})^{K_1-1}(1-e^{-\frac{y}{M_2}})^{K_2-1}dxdy=\sum_{i=0}^{K_1}\sum_{j=0}^{K_2-1}C_{K_1}^{i}C_{K_2-1}^{j}(-1)^{i+j}\frac{M_1K_2}{M_1+M_1j+M_2i}. \tag{27}$$

$$p_{s_l}^{R\to D}=\begin{cases}0, & K_2=0,\ 0<K_1\le K,\\ \sum_{i=0}^{K_1}\sum_{j=0}^{K_2-1}C_{K_1}^{i}C_{K_2-1}^{j}(-1)^{i+j}\frac{M_1K_2}{M_1+M_1j+M_2i}, & 0<K_1\le K,\ 0<K_2\le K,\\ 1, & K_1=0,\ 0<K_2\le K.\end{cases} \tag{28}$$

is the outage performance for $L\to\infty$ which shows the best potential performance for the max-ratio scheme.

First we consider Case 2. Because $M_1=M_2$, the probabilities to select a source-to-relay and relay-to-destination link are the same, and both equal $1/(K_1+K_2)$. This is similar to the max-link scheme in [25]. Thus building upon the analysis in [25], we can obtain that, if $L\to\infty$, the stationary probability for any state corresponding to $K_1\neq K$ or $K_2\neq K$ must be 0, or we have

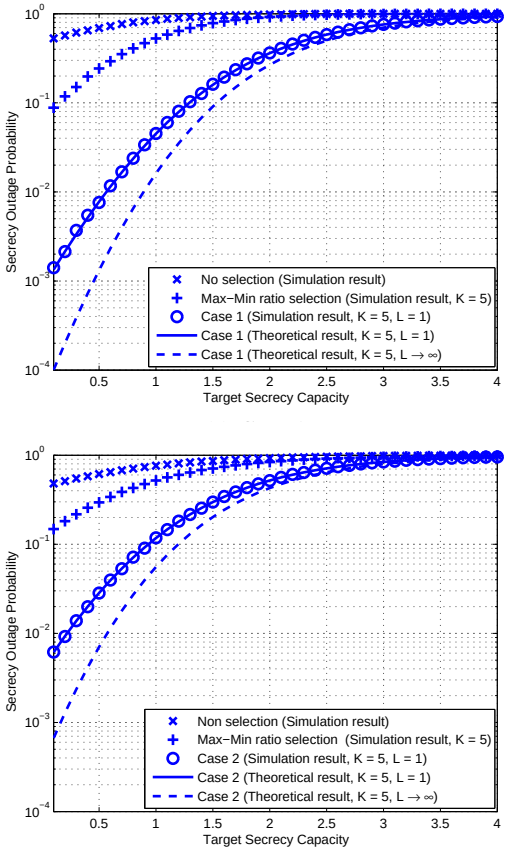
$$\sum_{s_l:K_1=K_2=K}P(s_l)=1. \tag{29}$$

This implies that, if $L\to\infty$, at any time, the best link is always selected from $K_1+K_2=2K$ available channels with the max-ratio scheme in Case 2.

In Case 1, unfortunately, we cannot have a simple form as in (29) for $L\to\infty$, because the probabilities to select a source-to-relay and relay-to-destination link are not equal, even with $M_1=M_2$. In order to illustrate the performance for $L\to\infty$, the original scheme can be assumed to be equivalent to a virtual relay section scheme having equal probability to select a source-to-relay and relay-to-destination link, or $P(x<y)=0.5$ where x and y are defined in Section IV-A. Then in the virtual scheme with $L\to\infty$, the number of available source-to-relay and relay-to-destination links are always K_1' and K_2', respectively, or $\sum_{s_l:K_1=K_1',K_2=K_2'}P(s_l)=1$. If we let $K_1'=K$, then K_2' can be obtained by solving $P(x<y)=0.5$ as (30) in the top of the next page, where $P(x<y)$ is given by (35) in the Appendix I.

Since K_2' obtained from (30) is usually not an integer, the virtual selection scheme cannot be realized in practice. However, it provides interesting insight in understanding the secrecy performance of the original max-ratio scheme in Case 1 for $L\to\infty$. Normally, we have $K_2'<K$, which implies that, on the average, the best link is always selected from $K_1'+K_2'$ available channels at any time and $K\le K_1'+K_2'\le 2K$.

For both Case 1 and 2, with a limited buffer size L, we always have $K_1+K_2\ge K$ at any time. On the contrary, in the max-min-ratio selection scheme, the best link is selected from only K links. Therefore, it follows that the max-ratio scheme has significantly better secrecy outage performance than the benchmark max-min-ratio scheme, and the best potential performance for the max-ratio scheme is reached when $L\to\infty$. This will be verified the next section.



(b) Case 2

Fig. 2. The secrecy outage probabilities for different relay selection schemes.

$$P(x<y)=\sum_{i=1}^{K_1'} C_{K_1'}^{i}(-1)^{i+1}K_2'(\frac{M_1}{M_2 i})^{K_2'}\mathcal{B}(2,K_2')\mathcal{F}_{2,1}([K_2'+1,K_2'],K_2'+2,1-\frac{M_1}{M_2 i})=0.5, \quad (30)$$

VII. Numerical Results

In this section, simulation results are given to verify the secrecy outage probabilities for the proposed max-ratio relay selection scheme. Both Case 1 and 2 are considered. In the simulation, all noise variance and transmission powers are normalized to unity, and the average channel gains for source-to-relay and relay-to-destination transmissions are set as $\gamma_{sr} = \gamma_{rd} = 30$ dB. Thus the corresponding average channel SNR is also 30 dB which is high enough to guarantee successful decoding at the relays and destination. The average eavesdropping channel gains, i.e. γ_{se} and γ_{re}, are determined through the settings of the average gain ratios $M_1 = \gamma_{sr}/\gamma_{se}$ and $M_2 = \gamma_{rd}/\gamma_{re}$, where we let $M_1 = M_2$ for various values in the simulations.

In every simulation below, both theoretical and simulated secrecy outage probabilities are shown to essentially perfectly match, where the theoretical results are based on (10) and simulation results are obtained by averaging $5,000,000$ independent runs. This verifies the closed-form secrecy outage probabilities obtained in this paper.

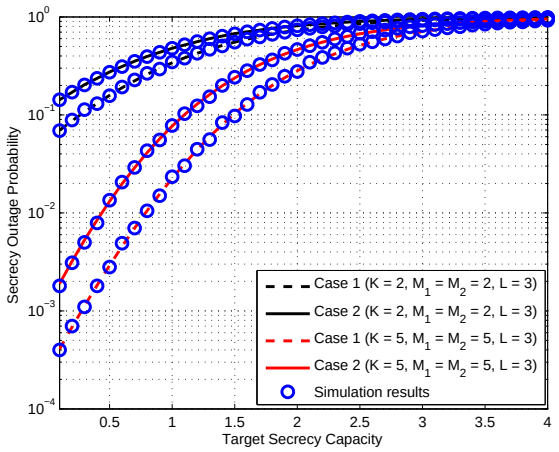
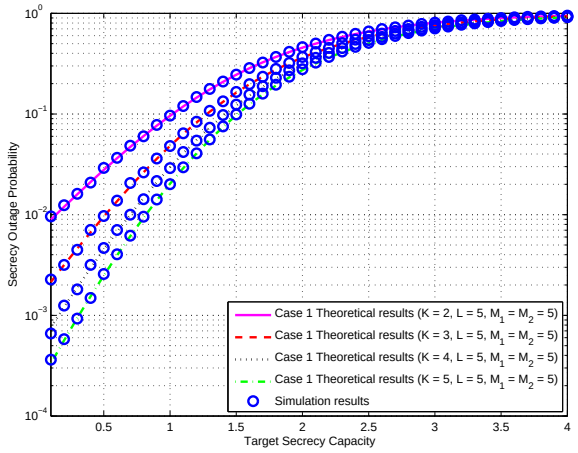
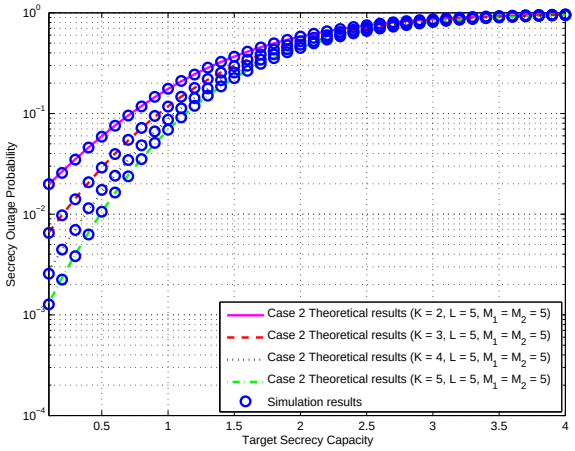


Fig. 3. The secrecy outage probabilities of the max-ratio scheme for Cases 1 and 2.

Fig. 2 compares the secrecy outage performance of the proposed max-ratio scheme with those for the no relay selection and the traditional max-min-ratio schemes, where the relay number is set as $K = 5$ in all relay selection schemes. It is clearly shown that the no relay selection scheme has the worst outage performance and the proposed max-ratio has the best. It is interesting to observe that, for both Cases 1 and 2, with buffer size $L = 1$, the max-ratio still performs significantly better than the max-min-ratio scheme. We highlight that the max-min-ratio scheme is effectively also equipped with a buffer of size 1, because the relays need to store the decoded data at one time and transmit out at the next time. However, even with $L = 1$, the max-ratio does not reduce to the max-min-ratio scheme. This is because, for any relay receiving a data packet in the max-ratio scheme, it has the choice of whether to transmit the packet out at the next time or not. On the contrary, the relays in the max-min-ratio schemes do not have such choices. Therefore, the max-ratio scheme has "coding gain" over the max-min-ratio approach. On the other hand, with $L \to \infty$, the best potential performance of the max-ratio is reached, which is clearly shown in Fig. 2 (a) and (b) for both Case 1 and 2 respectively.



(a) Case 1



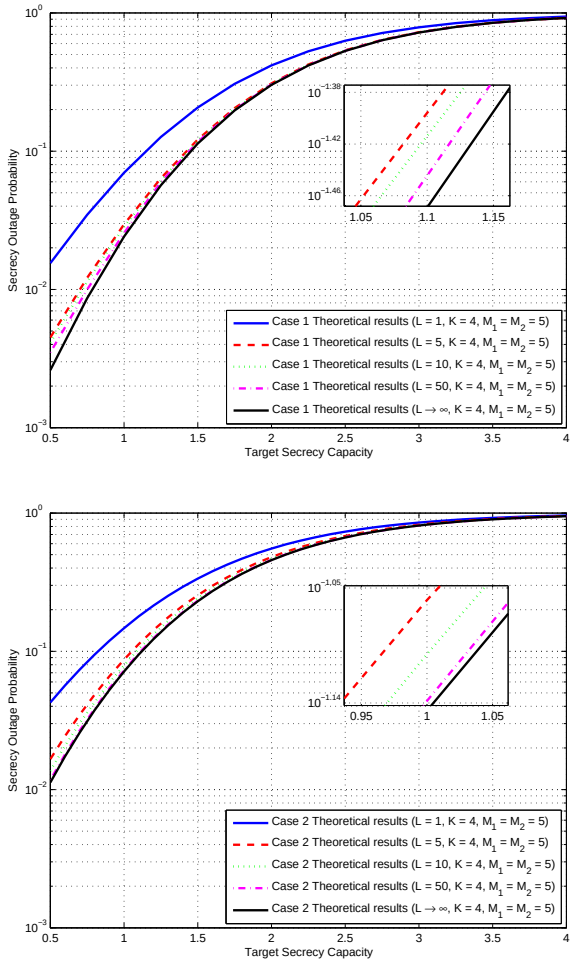
(b) Case 2

Fig. 4. The secrecy outage probabilities of the max-ratio scheme for different relay numbers K.

Fig. 3 compares the secrecy outage probabilities of the max-ratio scheme for Cases 1 and 2, where the buffer size is fixed at $L = 3$, the average gain ratios are set as $M_1 = M_2 = 2$ or 5, and the relay number is set as $K = 2$ or 5. It is clearly shown that the max-ratio scheme in Case 1 has consistently better performance than that in Case 2.

Fig. 4 compares the secrecy outage probabilities of the

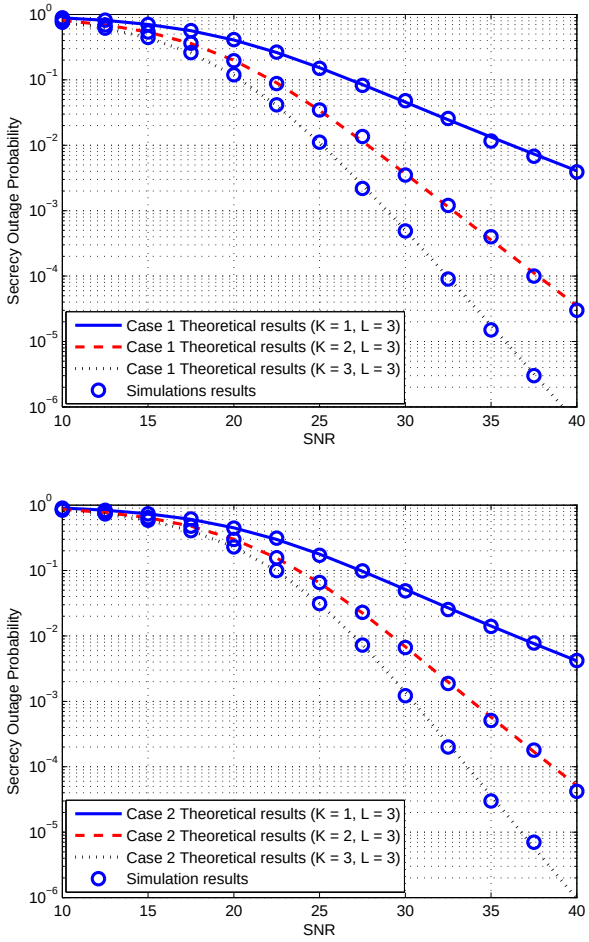
max-ratio scheme for different numbers of relays, where the buffer size is fixed as $L = 5$ and the average gain ratios are set as $M_1 = M_2 = 5$. It is clearly shown that, in both cases, the increase of the relay number can significantly improve the secrecy outage performance. For example, for the target secrecy capacity $\gamma_{sc} = 0.5$, when the relay number is increased from $K = 2$ to $K = 5$, the secrecy outage probability decreases by approximately 10 dB in Case 1, and by almost 6 dB in Case 2. This verifies the effectiveness of using the max-ratio relay selection in improving the secrecy performance.



(b) Case 2

Fig. 5. The secrecy outage probabilities of the max-ratio scheme for different relay buffer sizes L.

Fig. 5 compares the secrecy outage probabilities of the max-ratio scheme for different relay buffer sizes, where the relay number and average gain ratio are fixed at $K = 4$ and $M_1 = M_2 = 5$, respectively. While both the theoretical and simulation results have been obtained and perfectly match each other, only the theoretical results are shown in Fig. 5 as otherwise it would be too congested for illustration. Particularly, for $L \to \infty$ in Case 1, K_1' and K_2' for the virtual selection scheme (described in Section VI) are obtained as $K_1' = K = 4$ and $K_2' \simeq 2.23$ respectively. The theoretical result for Case 1 is then obtained by using $K_1' = 4, K_2' \simeq 2.23$ to calculate the outage probability in (10). On the other hand, the theoretical result for $L \to \infty$ in Case 2 is obtained by using $K_1 = K_2 = K = 4$ in the corresponding outage probability expression. In both Cases 1 and 2, for $L \to \infty$, the simulation results are actually obtained by using a very large buffer size $L = 500$. It is clearly shown that, for both Cases 1 and 2, the secrecy outage probability decreases with the increase of the buffer size L, but the improvement becomes less significant as L increases. In fact, when $L = 50$, the secrecy outage probability is already very close to that for $L \to \infty$.



(b) Case 2

Fig. 6. The secrecy outage probabilities *vs* SNR, where $\gamma_{se} = \gamma_{re} = 30$ dB and target secrecy capacity is unity.

Fig. 6 shows the secrecy outage probabilities *vs* the SNR for the proposed max-ratio scheme. It is clear that, in both Cases 1 and 2, the secrecy outage probability improves significantly with increased number of the relay nodes.

VIII. Conclusions

This paper proposed a new max-ratio relay selection policy for secure buffer-aided cooperative DF networks. With the help of buffers at the relays, the best relay was selected with the largest gain ratio among all available source-to-relay and relay-to-destination links. Both cases with knowledge of exact and average gain for eavesdropping links were considered, and for

the first time, in the challenging secure transmission context, closed-form expressions for the secrecy outage probabilities for both cases were derived. Both analysis and simulations show that the proposed max-ratio relay selection has significantly better performance in secrecy outage probability than the benchmark max-min-ratio scheme, and provides an attractive way to realize and improve secure transmission at the physical layer of wireless communications.

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers and the editor for their constructive comments.

APPENDIX I - PROOF OF (17)

Noting the definition of x and y in Section IV-A, we have

$$p_{s_l}^{R\to D} = P(x<y) = \int\int_{x<y} f_{XY}(x,y)dxdy = \int_0^\infty \int_0^y f_{XY}(x,y)dxdy, \tag{31}$$

where $f_{XY}(x,y)$ is the joint PDF of x and y.

From the CDF-s of x and y given by (13) and (14) respectively, the PDF-s of x and y are obtained as

$$f_X(x) = \sum_{i=0}^{K_1} \frac{C_{K_1}^i(-1)^{i+1}M_1 i}{(M_1+ix)^2} \quad \text{and} \quad f_Y(y) = \frac{y^{K_2-1}K_2M_2}{(M_2+y)^{K_2+1}}, \tag{32}$$

respectively. Because x and y are mutually independent, we have

$$f_{XY}(x,y) = f_X(x)f_Y(y) = \sum_{i=0}^{K_1} \frac{C_{K_1}^i(-1)^{i+1}M_1M_2K_2iy^{K_2-1}}{(M_1+ix)^2(M_2+y)^{K_2+1}}. \tag{33}$$

Substituting (33) into (31) gives

$$p_{s_l}^{R\to D} = \int_0^\infty \int_0^y \sum_{i=0}^{K_1} \frac{C_{K_1}^i(-1)^{i+1}M_1M_2K_2iy^{K_2-1}}{(M_1+ix)^2(M_2+y)^{K_2+1}}dxdy$$
$$= 1 + \sum_{i=1}^{K_1} C_{K_1}^i(-1)^i M_1M_2K_2 \int_0^\infty \frac{y^{K_2-1}}{(M_1+iy)(M_2+y)^{K_2+1}}dy. \tag{34}$$

Then according to [38], if $K_2>1$, we obtain

$$p_{s_l}^{R\to D} = 1 + \sum_{i=1}^{K_1} C_{K_1}^i(-1)^i K_2 \left(\frac{M_1}{M_2 i}\right)^{K_2} \mathcal{B}(2,K_2) \mathcal{F}_{2,1}\left([K_2+1,K_2], K_2+2, 1-\frac{M_1}{M_2 i}\right); \tag{35}$$

if $K_2=1$ and $M_1=M_2$, we have

$$p_{s_l}^{R\to D} = 1 - K_1/2 + \sum_{i=2}^{K_1} C_{K_1}^i(-1)^i \frac{i[\ln(i)-1]+1}{(i-1)^2}; \tag{36}$$

and if $K_2=1$ and $M_1\neq M_2$, we have

$$p_{s_l}^{R\to D} = 1 + \sum_{i=1}^{K_1} C_{K_1}^i(-1)^i M_1 \frac{i\ln(i)M_2 + i\ln(M_2)M_2 - i\ln(M_1)M_2 - iM_2 + M_1}{(M_1-iM_2)^2}. \tag{37}$$

REFERENCES

[1] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Jan. 1975.

[3] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[5] S. K. L. Y. Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[7] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[8] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[9] I. Csiszr and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[10] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[11] A. Papadogiannis, H. Bang, D. Gesbert, and E. Hardouin, "Efficient selective feedback design for multicell cooperative networks," *IEEE Trans. Veh. Technology*, vol. 60, pp. 196–205, Jan. 2011.

[12] Y. J. Fan, C. Wang, J. Thompson, and H. V. Poor, "Recovering multiplexing loss through successive relaying using repetition coding," *IEEE Trans. Wireless Commun.*, vol. 6, no. 12, pp. 4484–4493, Dec. 2007.

[13] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-Aided cooperation," *IEEE Trans. Inform. Forensics and Security*, vol. 4, no. 2, pp. 242 – 256, June. 2009.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *in Proc. 46th Ann. Allerton Conf. Communication, Control, and Computing, UIUC, Illinois*, Sep. 2008.

[15] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Taipei, Taiwan*, Apr. 2009.

[16] E. Tekin and A. Yener, "Themultiple access wire-tap channel:wireless secrecy and cooperative jamming," *in Proc. Information Theory and Applications Workshop, San Diego, CA*, Jan. 2007.

[17] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[18] Z. Ding, M. Peng, and H. H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[19] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.

[20] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[21] G. Chen, V. Dwyer, I. Krikidis, J. S. Thompson, S. McLaughlin, and J. A. Chambers, "Comment on 'Relay selection for secure cooperative networks with jamming'," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2351–2351, June 2012.

[22] J. C. Chen, R. Q. Zhang, L. Y. Song, Z. Han, and B. L. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[23] Z. Ding, Y. Gong, T. Ratnarajah, and C. Cowan, "On the performance of opportunistic cooperative wireless networks," *IEEE Trans. Commun.*, vol. 56, no. 8, pp. 1236–1240, Aug. 2008.

[24] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[25] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, May 2012.

[26] H. Liu, P. Popovski, E. Carvalho, and Y. Zhao, "Sum-rate optimization in a two-way relay network with buffering," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 95–98, Jan. 2013.

[27] A. Ikhlef, D. S. Michalopoulos, and R. Schober, "Max-max relay selection for relays with buffers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1124–1135, May 2012.

[28] N. Zlatanov, R. Schober, and L. Lampe, "Buffer-aided relaying in a three node network," *in Proc. 2012 IEEE International Symposium on Information Theory Proceedings, Cambridge, Massachusetts, USA*, pp. 781–785, July 2012.

[29] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2012.

[30] B. Xia, Y. Fan, J. Thompson, and H. V. Poor, "Buffering in a three-node relay network," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492–4496, Nov. 2008.

[31] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[32] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environment," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.

[33] K. Hamdi, W. Zhang, and K. B. Letaief, "Power control in cognitive radio systems based on spectrum sensing side information," *IEEE Intl. Conf. Commun.*, Glasgow, UK, June 2007.

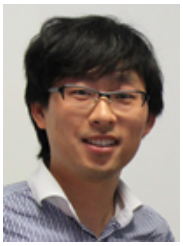
[34] C. M. Grinstead and J. L. Snell, "Introduction to probability: Second revised edition, Chapter11 Markov chains," *American Mathematical Society*, 1991.

[35] J. R. Norris, "Markov chains," *Cambridge University Press*, 1998.

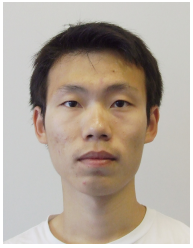
[36] A. Berman and R. J. Plemmons, "Nonnegative matrices in the mathematical sciences," *Society of industrial and applied mathematics*, 1994.

[37] H. A. David, "Order statistics second edition," *John Wiley Sons Ltd*, 1981.

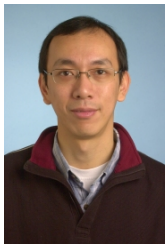
[38] I. S. Gradshteyn and I. M. Ryzhik, "Table of integrals, series, and products," *Elsevier Academic Press*, 7th ed. 2007.



Gaojie Chen (S'09-M'12) received the B. Eng. and B. Ec. in Electrical Information Engineering and International Economics and Trade from the Northwest University, Shaanxi, China, in 2006, and the M.Sc (Distinction) and Ph.D degrees from Loughborough University, Loughborough, UK, in 2008 and 2012, respectively, all in Electrical and Electronic Engineering. From 2008 to 2009 he worked, as a software engineering in DTmobile, Beijing, China, and from 2012 to 2013 as a Research Associate in the School of Electronic, Electrical and Systems Engineering at the Loughborough University, Loughborough, UK. He is currently a Research Fellow in the Faculty of Engineering and Physical Sciences at the University of Surrey, Guildford, UK. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio and secrecy communications.



Zhao Tian (S'12) received the B. Eng. degree in School of Electronic, Electrical and Systems Engineering from Loughborough University, UK, in 2012 He is currently working toward the Ph.D. degree in Advanced Digital Signal Process Group in School of Electronic, Electrical and Systems Engineering from Loughborough University, UK with full postgraduate scholarship from Engineering and Physical Sciences Research Council (EPSRC). His current research interest include the general field of wireless communications with emphasis on buffer-aided relaying.



Yu Gong is with School of Electronic, Electrical and Systems Engineering, Loughborough University, UK, in July 2012. Dr Gong obtained his BEng and MEng in electronic engineering in 1992 and 1995 respectively, both at the University of Electronics and Science Technology of China. In 2002, he received his PhD in communications from the National University of Singapore. After PhD graduation, he took several research positions in Institute of Infocomm Research in Singapore and Queens University of Belfast in the UK respectively. From 2006 and 2012, Dr Gong had been an academic member in the School of Systems Engineering, University of Reading, UK. His research interests are in the area of signal processing and communications including wireless communications, cooperative networks, non-linear and non-stationary system identification and adaptive filters.

Zhi Chen (M'04) received B. Eng, M. Eng., and Ph.D. degree in Electrical Engineering from University of Electronic Science and Technology of China (UESTC), in 1997, 2000, 2006, respectively, all in electrical engineering. After his Ph.D. graduation, he joined the National Key Lab of Science and Technology on Communications, UESTC, where he was promoted to Professor in August 2013.. He was a visiting scholar at University of California, Riverside during 2010-2011. His current research interests include wireless communication and signal processing, specifically relay and cooperative communications, interference coordination and cancellation. Dr. Chen has served as a reviewer for various international journals and conferences, including IEEE Transactions on Signal Processing, IEEE Transactions on Vehicular Technology, and many more.

Jonathon A. Chambers (S'83-M'90-SM'98-F'11) received the Ph.D. and DSc degrees in signal processing from the Imperial College of Science, Technology and Medicine (Imperial College London), London, U.K., in 1990 and 2014. From 1991 to 1994, he was a Research Scientist with the Schlumberger Cambridge Research Center, Cambridge, U.K. In 1994, he returned to Imperial College London, as a Lecturer in signal processing and was promoted as a Reader (Associate Professor) in 1998. From 2001 to 2004, he was the Director of the Centre for Digital Signal Processing and a Professor of signal processing with the Division of Engineering, King's College London, London. From 2004 to 2007, he was a Cardiff Professorial Research Fellow with the School of Engineering, Cardiff University, Wales, U.K. In 2007, he joined the Department of Electronic and Electrical Engineering, Loughborough University, Loughborough, U.K., where he heads the Advanced Signal Processing Group and serves as the Associate Dean (Research) for Loughborough University in London. He is a coauthor of the books Recurrent Neural Networks for Prediction: Learning Algorithms, Architectures and Stability (New York, NY, USA: Wiley, 2001) and EEG Signal Processing (New York, NY, USA: Wiley, 2007). He has advised more than 50 researchers through to Ph.D. graduation and published more than 350 conference proceedings and journal articles, many of which are in IEEE journals. His research interests include adaptive and blind signal processing and their applications. Dr. Chambers is a Fellow of the Royal Academy of Engineering, U.K., and the Institution of Electrical Engineers (IEE). He was the Technical Program Chair of the 15th International Conference on Digital Signal Processing and the 2009 IEEE Workshop on Statistical Signal Processing, both held in Cardiff, U.K., and a Technical Program Cochair for the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing, Prague, Czech Republic. He received the first QinetiQ Visiting Fellowship in 2007 for his outstanding contributions to adaptive signal processing and his contributions to QinetiQ as a result of his successful industrial collaboration with the international defense systems company QinetiQ. He has served on the IEEE Signal Processing Theory and Methods Technical Committee for six years, the IEEE Signal Processing Society Awards Board for three years and is currently a member of the IEEE Signal Processing Conference Board, and the European Signal Processing Society Best Paper Awards Selection Panel. He has also served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING for three terms over the periods 1997-1999, 2004-2007, and 2011- (and is currently a Senior Area Editor).